Лабораторная 3. Пакетные анализаторы трафика

Цель:

Приобрести навыки работы с пакетными анализаторами трафика

Задачи:

1. Подключится к виртуальной машине на облачной платформе СПбГУТ
2. Установить tcpdump
3. Получить навыки работы с tcpdump
4. Получить навыки работы с SCP
5. Получить навыки работы с Wireshark

Работа с анализатором пакетов tcpdump

tcpdump это компьютерная программа анализатор пакетов работающая через интерфейс командной строки. Она позволяет пользователю отображать пакеты, передаваемые или получаемые по сети

Синтаксис tcpdump

```
tcpdump {опции} -i {название интерфейса} {Фильтры}
```

опции tcpdump

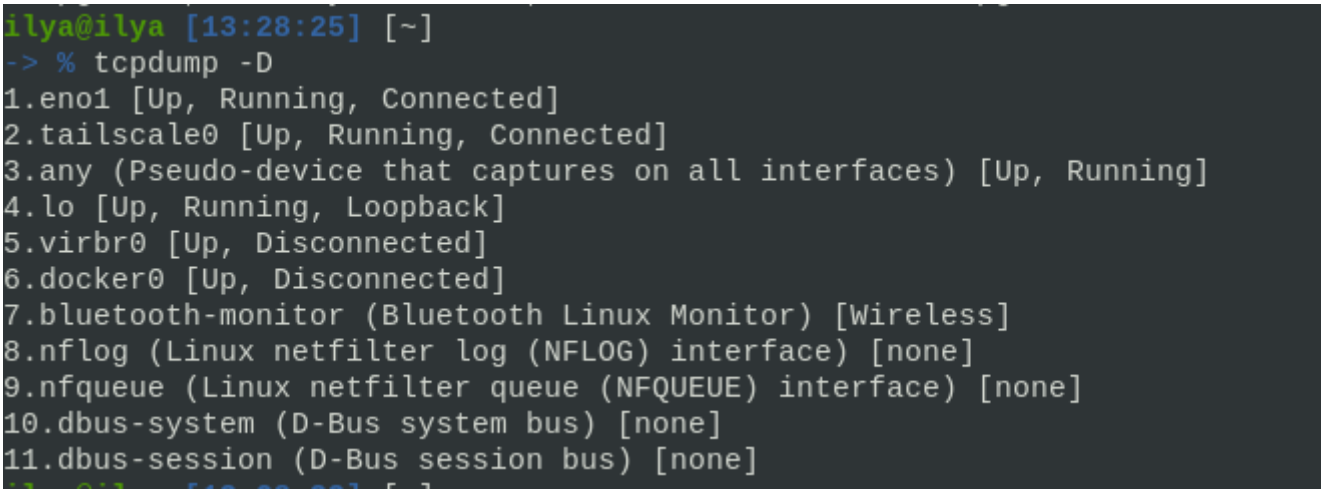
Ключ опции	Что делает
-A	Вывод пакетов в кодировке ASCI
-c n	перехватить n пакетов
-C n	создание дампа трафика определенного при размере, при генерации больше заданного создать новый файл для дампа, где n размер пакета по умолчанию указывается 1000000 байт Добавив к значению суффикс k/K, m/M или g/G, единицу измерения можно изменить на 1,024 (КиБ), 1,048,576 (МиБ) или 1,073,741,824 (ГиБ) соответственно.
-D	вывести список сетевых интерфейсов

Ключ опции	Что делает
-e	выводить информацию уровня соединения для каждого пакета, это может быть полезно, например, для отображения MAC адреса
-n	не отображать домены
-K	не проверять контрольные суммы пакетов
-w {название дампа}.pcap	запись вывода в файл
-r {название дампа}.pcap	чтение дампа созданного с помощью ключа -w
-v -vv -vvv	Более подробный вывод, желательно устанавливать -vvv, для дальнейшей работы
-q	выводить минимум информации

Примеры работы с tcpdump

Просмотр всех интерфейсов

```
sudo tcpdump -D
```



Просмотр всего трафика на интерфейсе `eno0` с адресом назначения `8.8.8.8`

```
sudo tcpdump -i eno0 ip dst 8.8.8.8
```

> Название интерфейса брать из своей конфигурации

```
ilya@ilya [17:25:21] [~]
-> % ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=103 time=5.58 ms
```

```
ilya@ilya [17:24:42] [~]
-> % pinh5~
ilya@ilya [17:24:43] [~]
-> %
ilya@ilya [17:24:58] [~]
-> % sudo tcpdump -i eno1 ip dst 8.8.8.8
[sudo] password for ilya:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:25:08.913243 IP ilya > dns.google: ICMP echo request, id 1, seq 21, length 64
17:25:09.915011 IP ilya > dns.google: ICMP echo request, id 1, seq 22, length 64
17:25:10.916719 IP ilya > dns.google: ICMP echo request, id 1, seq 23, length 64
17:25:11.918568 IP ilya > dns.google: ICMP echo request, id 1, seq 24, length 64
17:25:12.920374 IP ilya > dns.google: ICMP echo request, id 1, seq 25, length 64
17:25:13.922127 IP ilya > dns.google: ICMP echo request, id 1, seq 26, length 64
17:25:14.923760 IP ilya > dns.google: ICMP echo request, id 1, seq 27, length 64
17:25:15.925593 IP ilya > dns.google: ICMP echo request, id 1, seq 28, length 64
17:25:16.927515 IP ilya > dns.google: ICMP echo request, id 1, seq 29, length 64
17:25:17.929367 IP ilya > dns.google: ICMP echo request, id 1, seq 30, length 64
17:25:18.931152 IP ilya > dns.google: ICMP echo request, id 1, seq 31, length 64
17:25:19.932938 IP ilya > dns.google: ICMP echo request, id 1, seq 32, length 64
17:25:20.933882 IP ilya > dns.google: ICMP echo request, id 1, seq 33, length 64
17:25:21.723105 IP ilya > dns.google: ICMP echo request, id 2, seq 1, length 64
```

Просмотр всего трафика на интерфейсе `eno0` с адресом отправки `8.8.8.8`

```
sudo tcpdump -i eno0 ip src 8.8.8.8
```

> Название интерфейса брать из своей конфигурации

```
64 bytes from 8.8.8.8: icmp_seq=129 ttl=103 time=5.60 ms
64 bytes from 8.8.8.8: icmp_seq=130 ttl=103 time=5.37 ms
64 bytes from 8.8.8.8: icmp_seq=131 ttl=103 time=5.46 ms
64 bytes from 8.8.8.8: icmp_seq=132 ttl=103 time=5.41 ms
64 bytes from 8.8.8.8: icmp_seq=133 ttl=103 time=5.52 ms
64 bytes from 8.8.8.8: icmp_seq=134 ttl=103 time=5.59 ms
```

```
-> % sudo tcpdump -i eno1 ip src 8.8.8.8
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:26:51.881207 IP dns.google > ilya: ICMP echo reply, id 2, seq 91, length 64
17:26:52.883100 IP dns.google > ilya: ICMP echo reply, id 2, seq 92, length 64
17:26:53.884889 IP dns.google > ilya: ICMP echo reply, id 2, seq 93, length 64
17:26:54.886759 IP dns.google > ilya: ICMP echo reply, id 2, seq 94, length 64
17:26:55.888518 IP dns.google > ilya: ICMP echo reply, id 2, seq 95, length 64
17:26:56.890315 IP dns.google > ilya: ICMP echo reply, id 2, seq 96, length 64
17:26:57.892035 IP dns.google > ilya: ICMP echo reply, id 2, seq 97, length 64
```

Просмотр всего трафика на интерфейсе `eno0` с доменным именем назначения `resds.ru`

```
sudo tcpdump -i eno0 dst host  resds.ru
```

> Название интерфейса брать из своей конфигурации

```
rtt min/avg/max/mdev = 0.247/0.373/0.502/0.054 ms
ilya@ilya [17:31:14] [~]
-> % ping resds.ru
PING resds.ru (172.17.1.16) 56(84) bytes of data.
64 bytes from 172.17.1.16 (172.17.1.16): icmp_seq=1 ttl=64 time=0.258 ms
64 bytes from 172.17.1.16 (172.17.1.16): icmp_seq=2 ttl=64 time=0.364 ms
```

```
ilya@ilya [17:31:12] [~]
-> % sudo tcpdump -i eno1 dst host resds.ru
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:31:16.195074 IP ilya > 172.17.1.16: ICMP echo request, id 6, seq 1, length 64
17:31:17.196236 IP ilya > 172.17.1.16: ICMP echo request, id 6, seq 2, length 64
```

Просмотр всего трафика на интерфейсе `eth0` с доменном отправки `resds.ru`

```
sudo tcpdump -i eno0 dst host resds.ru
```

> Название интерфейса брать из своей конфигурации

```
ilya@ilya [17:37:04] [~]
-> % ping resds.ru
PING resds.ru (172.17.1.16) 56(84) bytes of data.
64 bytes from 172.17.1.16 (172.17.1.16): icmp_seq=1 ttl=64 time=0.283 ms
64 bytes from 172.17.1.16 (172.17.1.16): icmp_seq=2 ttl=64 time=0.240 ms
64 bytes from 172.17.1.16 (172.17.1.16): icmp_seq=3 ttl=64 time=0.380 ms
64 bytes from 172.17.1.16 (172.17.1.16): icmp_seq=4 ttl=64 time=0.375 ms
```

```
ilya@ilya [17:36:59] [~]
-> % sudo tcpdump -i eno1 src host resds.ru
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:37:08.108147 IP 172.17.1.16 > ilya: ICMP echo reply, id 7, seq 1, length 64
17:37:09.109336 IP 172.17.1.16 > ilya: ICMP echo reply, id 7, seq 2, length 64
17:37:10.111232 IP 172.17.1.16 > ilya: ICMP echo reply, id 7, seq 3, length 64
17:37:11.112852 IP 172.17.1.16 > ilya: ICMP echo reply, id 7, seq 4, length 64
```

Просмотр трафика на интерфейсу `eno0` с использованием `80` порта

```
sudo tcpdump -i eno0 port 80
```

> Название интерфейса брать из своей конфигурации



Просмотр трафика на интерфейсе `eth0` использующих диапазон портов `80-443`

```
sudo tcpdump -i eth0 portrange 80-443
```

Также для некоторых протоколов существуют готовые фильтры к примеру можно отфильтровать все `arp` пакеты интерфейса `eth0`

```
sudo tcpdump -i eth0 arp
```

Возможно фильтрация по размеру пакета, так мы можем отфильтровать все пакеты меньше 64 байт

```
sudo tcpdump -i eth0 less 64
```

Фильтрация пакетов больше 64

```
sudo tcpdump -i eth0 greater 64
```

Сохранить весь `udp` трафик проходящий интерфейс `eth0` в файл `dump.pcap`

```
sudo tcpdump -i eth0 udp -w dump.pcap
```

прочитать дамп `dump.pcap`

```
tcpdump -r dump.pcap
```

Использование SCP

SCP (secure copy) — это утилита командной строки, которая позволяет безопасно копировать файлы и каталоги между двумя локациями. Базовая технология для работы scp - это SSH(Secure Shell)

С помощью scp можно скопировать файл или каталог:

- От локальной машины к удаленной.
- От удаленной системы к вашей локальной машине.
- Между двумя удаленными системами.

Синтаксис SCP

```
scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2
```

Опции SCP

ключ	Что делает
-p	порт ssh на удаленной системе
-r	рекурсивное копирование
-C	Сжатие при передаче на удаленное устройство
-i n	использование ключа авторизации, где n путь к файлу ключа
-1	использовать SSH 1
-2	использовать SSH 2
-4	использовать IPv4
-6	использовать IPv6
-o ssh_option	Возможность использовать дополнительные опции реализованные в протоколе SSH, на месте ssh_option используется ключи используемые ssh клиентом
-q	Тихий режим ничего не выводится во время передачи

Примеры использования

Перемещение файла `foobar.txt` с узла `resds.ru` под пользователем `test` в локальную домашнюю директорию

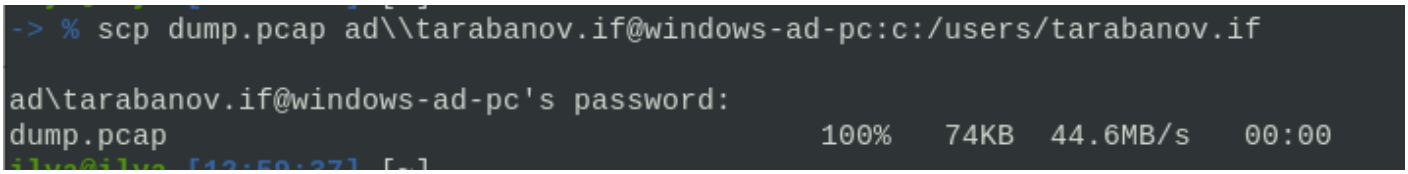
```
scp test@resds.ru:foobar.txt ~/
```

> “ является примером, не выполнять

Перемещение файла `dump.pcap` из текущей директории на компьютер с именем `windows-ad-pc` для пользователя `tarabanov.if` находящимся в домене `ad`, в домашнюю директорию пользователя

```
scp dump.pcap ad\\tarabanov.if@windows-ad-pc:c:/users/tarabanov.if
```

- windows-ad-pc - ip адрес вашего PC
- ad\tarabanov.if - учетная запись на вашем ПК
- c:/users/tarabanov.if - путь к директории, куда перемещается файл



Заданием scp

1. Создайте текстовый файл с вашими ФИО и группой и переместите его на локальный пк(аудиторный)

   > Группа ИКТК-XY
   >
   > Иванов Иван Иванович
   >
   > Петров Петр Петрович

2. создайте нового пользователя `test_scp` с паролем `password`
   1. смените пользователя на test_scp
   2. Создайте текстовый файл с названием лабораторной работы
   3. Вернуться на основную учетную запись
   4. передать с пользователя test_scp на локальный пк(аудиторный)

Задание

1. Открыть консольный мультиплексор
   1. Запустить снятие трафика, с записью трафика в файл `http.pcap`
   2. Разделить экран вертикально на половину
   3. Загрузить страницу, сделанную в первой лаб. работе
   4. Закончить снятие трафика
2. Передать файл на локальный(аудиторный пк)
3. Открыть файл в `wireshark`, отфильтровать для отображения только задействованных пакетов в передачи html страницы

Версия #23
Тарабанов Илья Федорович создал 16 сентября 2022 17:12:38
Тарабанов Илья Федорович обновил 17 октября 2023 14:10:49